UNIVERSITY OF HULL

File Storage Policy

Classification:	Policy
Version Number:	1.0
Status:	Approved
Approved by (Board):	Information Governance Committee
Approval Date:	19 April 2021
Effective from:	19 April 2021
Next Review Date:	Annual
Document Authors:	Steph Jones, Dan Chambers
Document Owner:	Head of Service Assurance, ICT (Stewart Doyle)
Department/Contact:	ICT
Summary:	This policy outlines the organisational responsibilities and controls around the storage of files within the University.
Scope:	This policy applies to all University members
Collaborative provision:	Not mandatory
Assessment: (where relevant)	Not applicable
Consultation: (where relevant)	Not applicable
Relevant legal frameworks:	See relevant section of overarching Information Governance and Assurance Policy
Related documents:	Information Governance and Assurance Policy, Data Protection Policy
Published locations:	Public website (www.hull.ac.uk)
Document Communication and Implementation Plan:	Available upon request.

All printed versions of this document are classified as uncontrolled.
A controlled version is available from the university website.

File Storage Policy

1. Introduction

1.1. This policy outlines the use of file storage within the University in order to protect data.

1.2. This policy supports the objectives of the overarching **Information Security Controls Policy**, as well as the **Data Protection Policy** and **Information Governance and Assurance Policy**.

2. Scope

2.1. This policy covers all devices used to conduct University related business, and any file storage methods.

2.2. This policy applies to all University members, third parties and visitors using University computer equipment.

2.3. For the purposes of this policy, "University data" refers to any data owned or licensed by the University that if disclosed publicly without authorisation, could result in financial, commercial or reputational damage and/or legal proceedings.

3. Local (fixed) disk drives

3.1. Local (fixed) disk drives (aka 'C: drive') on managed devices are for the primary purpose of storing the operating system and local profile settings for users. These should always be regarded as volatile – when a managed device is imaged it will overwrite any data on it.

3.2. Where exceptions exist such as the use of development software especially in teaching areas that are incompatible with network storage, then it is recommended that backups are facilitated using personal removal media or to cloud storage at regular intervals.

3.3. Local (fixed) disk drives should not be used for any storage of University or personal data. University data should always be stored on University network storage or approved University cloud storage services.

3.4. Local (fixed) disk drives should not be considered as secure.

3.5. ICT will reserve the right to refuse any request to attempt restoration of any University or personal data that has been lost by having been stored on local (fixed) disk drives.

4. Network storage

4.1. ICT provide centralised network storage for all University members. This is hosted and managed within the University data centre.

4.2. Network storage is subject to regular snapshot and backup provision with a retention period of 6 months.

4.3. Network storage is secured by authentication and access control, but is not encrypted. This should be sufficient for most business needs, however research data, for example, may have need to be encrypted. Guidance shall be available to University members.

4.4. Network storage is subject to quotas and must only be used for storing University data, and not for the purpose of personal photos, music, or videos.

4.5. A ‘home’ drive is provided for individual use and can only be accessed by the member of staff that it is provisioned for.

4.6. A set of ‘shared’ drives are also provided for departmental use as well as a shared drive for the sharing of student materials. Access to shared areas are controlled based on centralised group membership.

4.7. Each departmental area drive must have a designated owner. This will be set to the member requesting its creation, or where ownership has been transferred to them.

4.8. The designated owner agrees to comply with the University **Data Protection Policy** and accept their responsibilities for its ongoing management.

4.9. The designated owner is responsible for administering who can access the area. ICT shall provide a suitable mechanism to allow the owner capability to administer group membership.

4.10. In the event that a designated owner, or the line manager of that owner, needs to arrange cover for planned or unplanned absence, the owner or line manager should request temporary or permanent transfer of ownership through ICT.

4.11. In the event that a University member assigned as owner changes role or leaves the institution, they must ensure that ownership is transferred through ICT.

4.12. Should a shared area owner be assigned in error, the owner should contact ICT.

4.13. All owners will be notified on a quarterly basis to review the current membership of that shared area.

4.14. University members must notify ICT if they know or suspect that any data has been breached or data is inappropriate for shared areas. If personal data is involved, the procedures in the **Data Protection Policy** must be followed.

5. Cloud storage

5.1. Only University approved cloud storage services must be used for the storing of University data. ICT currently provide cloud storage through Box and OneDrive.

5.2. Box and OneDrive both provide encrypted storage.

5.3. A majority of University members are eligible for an ICT provisioned cloud storage account.

5.4. Cloud storage allows for collaborative working. When sharing files, always check that the intended members are the ones to be invited.

5.5. Caution should always be exercised when sharing files through public links. These are not restricted to University members and anyone who is in possession of the link can access the shared files.

5.6. In the event that a University member changes role or leaves the institution, and are an owner of files that have been previously shared, they must ensure that ownership of files are transferred to another appropriate member before they do so.

5.7. When a University member leaves the institution, their cloud storage account will be closed and then deleted after a period of 3 months.

5.8. In the event of a line manager needing to gain access to files held in a cloud storage account after its closure will need to be risk-assessed and authorised in accordance with the University **Data Protection Policy**.

5.9. Box storage adheres to the EU Safe Harbour Framework, however, data is held outside of the UK and Europe. OneDrive storage is held within the EU zone.

5.10. If there is a need to store personal data on Box, then this must be done in accordance with the University **Data Protection Policy**.

5.11. University members must notify ICT if they know or suspect that any data has been breached through the use of Box, OneDrive, or other cloud storage services. If personal data is involved, the procedures in the **Data Protection Policy** must be followed.

6. Removable media

6.1. Removable media refers to any type of digital storage that is not physically fixed inside a device. This includes, but is not limited to: USB flash drives (aka 'memory sticks', pens), external hard disk drives, phones using SD card storage, and optical media (e.g. DVD, CD).

6.2. Removable media provide a common route for the introduction of malware and the accidental or deliberate export of sensitive data. In the normal course of business, it should not be necessary to use removable media, and the risk of doing so usually outweighs any perceived benefit.

6.3. Removable media is very easily lost, which can, and does, result in the breach of data.

6.4. Removable media that is used to transfer information from one device to another, for example a University PC to one at home, can be utilised by attackers to transport malicious software from one environment to the other.

6.5. The use of removable media within the University is not prohibited, but should only be used in cases where no suitable alternative exists (e.g. ICT network shares/cloud storage).

6.6. Managers and information asset owners shall ensure that use of removable media is suitably controlled within their area of responsibility in line with the objectives of this policy.

6.7. University staff members within professional services electing to use removable media, shall be responsible for ensuring they are authorised to do so within their area.

6.8. Any removable media used by staff to transport or store any University data should be purchased via approved channels.

6.9. Personally owned removable media shall not be used by staff for the purposes of transporting or storing University data.

6.10. Guidance on encryption including recommended hardware and software shall be available to University members.

6.11. Researchers are responsible for ensuring that use of removable media and the encryption of any such media meets the requirements imposed upon them by their research (e.g. by funders, or data sharing agreements).

6.12. Use of removable media by a third party or sub-contractor should be risk-assessed and authorised, and in accordance with University **Data Protection Policy** governing third-party access to data.

6.13. It is recommended that removable media be made externally identifiable where possible (e.g. using a fob/tag or to note the owners name/contact number).

6.14. When the removable media has reached the end of its useful life it should be submitted to the ICT department for secure destruction.

6.15. If removable media has been lost, it should be reported to the Campus Security team.

6.16. If removable media has been found, it should be handed in to the Campus Security team. If identifiable (from a description/external labelling) then attempts will be made to return to its owner. If this is not the case, removable media must never be inserted into a device in order to try and identify its owner, as this can present a security risk.

6.17. Any unidentifiable removable media that has not been claimed within six months will be submitted for secure destruction.